REMARKS

Claims 1-8 and 13-19 are pending in the Application. Claims 1-2, 4-6, 8, 13-14, and 16-19 are amended. For the following reasons, this application should be considered in condition for allowance and the case passed to issue.

Claims 1, 2, 5, 6, 13, and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Gillon et al., U.S. Patent 5,838,927, in view of Elgamal et al., U.S. Patent 5,657,390, Shaffer et al., U.S. Patent 5,784,461, and either Finkelstein et al., U.S. Patent 5,319,712 or Zuquete et al. This rejection is respectfully traversed. The following is a comparison between applied reference and the claimed invention.

The present invention relates to a method for providing communication protocol layer independent security for data transmitted between two network nodes. The method comprises the steps of establishing communication between the two nodes, and in response to the establishment of the communication between the two nodes encrypting data and sending the data from the first node to the second node. The encrypting of the data is performed independent of any communication protocol layers used to transport the encrypted data. The data is decrypted at the second node in response to the encrypted data being read from the second node. One patentable feature of the present invention is that the decrypting and encrypting of data is performed independent of any communication protocol layers used to transfer the encrypted data from the first network node to the second network node.

Gillon et al., discloses a method of apparatus for compressing a continuous indistinct data stream. Figure 6 of Gillon et al. is a flow chart of the layering of the protocol layers used to send data over the internet. As shown in block 602, a data stream is received from a remote source or from a local disk. The data is analyzed, compressed and attached to a compression stream; the

compression stream is the second layer of communication protocol with the data stream being the first layer. The data is then attached to other types of streams, for example an encryption stream, shown in block 608. The encryption stream is another layer in the communication protocol layers of Gillon et al. The encryption stream is attached to a write stream in block 610. The write stream is a lower layer in the communication protocol layers of Gillon et al. The write stream is transmitted with the attached streams over the internet and received by the client. Figure 4B shows the layering of the data stream layer, the compression stream layer, and the encryption stream layer prior to transmission. Figure 4C shows the reverse layering of the encryption stream layer, the compression stream layer, and data stream layer as the data is received after transmission. Gillon et al. clearly teaches that the encryption stream layer is dependent on the compression stream layer and the data stream layer. In the communication protocol layers of Gillon et al., a data stream layer is established and compressed into a compression stream layer. The compressed data stream layer is encrypted into an encryption stream layer; the encrypted data is not independent of all other layers of the communication protocol layers. This is unlike the present invention as claimed in independent claims 1, 5, 13, and 17. The present invention requires that the encrypting of data be performed independent of any communication protocol layers used to transport the encrypted data.

Elgamal et al. teaches the computer network that encrypts and decrypts information transferred over a network. Elgamal et al. teaches a security protocol layer between an application layer and a transport layer. The application layer is communication protocol layer. In column 5 line 17, Elgamal et al. teaches that the application protocol layer used by the application program is used to communicate over a network. The present invention is distinguishable from Elgamal et al. as this security protocol layer is beneath the application

protocol layer. The present invention as claimed in independent claims 1, 5, 13, and 17 require the encrypting of the data is performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node. It is well known in the art that a layer that is beneath another layer is dependent on the above layer.

Shaffer et al. relates to a secure method for granting customer access to images and image related services in an image fulfillment center. Shaffer et al. is primarily concerned with the exchange of encryption security key between a vendor and a customer located at different locations for the encryption of photographs. As discussed in column 5 lines 31-38, a customer uses a security key associated with the image to encrypt a request for services relating to that image. The customer then sends the encrypted request along with the encrypted I.D. relating to the image to the fulfillment center. The encrypted request for services is independent of the underlying protocol(s) used to establish communication data transfer connection with the fulfillment center. The present invention as claimed in independent claims 1, 5, 13, and 17 is distinguishable from Shaffer et al. as Shaffer et al. do not disclose encryption of data stream, but rather uses encryption to authenticate the request for a high resolution image. Shaffer et al. does not teach any specifics of the communication protocols between a customer and a fulfillment center in the hierarchy of the communication layers in association with the encryption layer. The Shaffer et al. teaching of "underlying protocol(s)" merely exhibits that Shaffer et al. recognizes different communication protocols are layered.

Finkelstein et al., is related to a method and apparatus for providing cryptographic protection of a data stream. Finkelstein et al. is distinguishable from the present invention as claimed in independent claims 1, 5, 13, and 17 as the encryption is dependent on other communication protocol layers as shown in Figure 1 as the encryption layer 2 is between layers 1

and 3. The encryption of Finkelstein et al. is therefore not independent of all communication protocol layers.

Zuquete et al., is an article that teaches privacy enhanced sockets, the sockets of which are a layer of Zuquete's communication channels.

None of the references (Gillon et al., Elgamal et al., Shaffer et al., Finkelstein et al., or Zuquete et al.) used to reject claims 1, 2, 5, 6, 13, and 14 teach the limitation of encrypting data independent of any communication protocol layer used to transport the encrypted data from the first network node to the second network node, as claimed in independent claims 1, 5, 13, and 17. Additionally, none of these references disclose that the encryption is done in response to data being written into a first stream, which is required by independent claims 1, 5, 13, and 17. For these and other reasons, claims 1, 2, 5, 6, 13, and 14 are distinguishable over the cited prior art and the rejection under 35 U.S.C. § 103(a) should be reconsidered and withdrawn. The rejections of claims 3, 4, 7, 8, 15, and 16 under 35 U.S.C. § 103(a) should also be reconsidered and withdrawn as the cited prior art fails to teach the encryption of data independent of any communication protocols in independent claims 1, 5, and 13 of which claims 3, 4, 7, 8, 15, and 16 depend from.

Claim 17 was rejected under 35 U.S.C. 103(a) as being unpatentable over Gillon et al., U.S. Patent 5,838,927 in view of Elgamal et al., U.S. Patent 5,657,390, Shaffer et al., U.S. Patent 5,784,461, and either Finkelstein et al., U.S. Patent 5,319,712 or Zuquete et al. As discussed in the Response to the rejection of claims 1, 2, 5, 6, 13, and 14, none of the applied references teach the limitation of encrypting the data independent of any communication protocol layer used to transport the encrypted data on a communication channel, as claimed in claim 17. For these

reasons and others, claim 17 is distinguishable from the cited prior art and the rejection under 35 U.S.C. § 103(a) should be reconsidered and withdrawn.

The rejection of claims 18 and 19 under 35 U.S.C. § 103(a) should also be reconsidered and withdrawn as cited prior art in the rejection of claim 17 from which claims 18 and 19 depend from, fails to teach the limitation of the encryption of data being independent of any communication protocol layer used to transport encrypted data on a communication channel. For above reasons and other reasons, claims 18 and 19 are distinguishable from the prior art and the rejection under 35 U.S.C. § 103(a) should be reconsidered and withdrawn.

In view of the above, it is believed that this application is in condition for allowance, such a notice is respectfully solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Daniel H. Sherr
Registration No. P-46,425

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 DHS:MWE
Date: April 28, 2000
Facsimile: (202) 756-8087